Department of
INFORMATION
TECHNOLOGY

Maryland Boundary Protection and Internet Access Policy

Last Updated: 01/31/2017

Contents

1.0 Purpose

The establishment of perimeter defense mechanisms is an important part of minimizing exposure to security threats. The Maryland Department of Information Technology (DoIT) is committed to managing the confidentiality, integrity, and availability of State information technology networks, systems and applications (IT Systems). This includes establishing security controls for the boundaries between the DoIT Enterprise and subordinate agency networks, or between the DoIT Enterprise and 3rd party networks including the Internet. The Maryland Department of Information Technology (DoIT) will utilize baseline controls and standards established by NIST SP 800-53R4, NIST SP 800-41R1, and NIST SP 800-94 to develop this policy.

2.0 Document and Review History

This policy supersedes the DoIT Firewall Policy (version 2.0, May 2013) and any other related policy concerning boundary protection and firewall devices declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is applicable to all networks utilized by any agency supported by, or under the policy authority of, the Maryland Department of Information Technology.

4.0 Policy

The Maryland Department of Information Technology shall establish controls that monitor and manage the flow of information of any agency supported by, or under the policy authority of, DoIT. These controls will govern the flow of information within the internal network (intranet) and at all external boundaries of the information systems and networks the agencies operate.

The Secretary of Information Technology shall designate the Director of Cybersecurity or a designated State employee to oversee management and administration of secure network boundary protection devices (such as routers, switches, **firewalls**, and other boundary protection devices) for Enterprise onboarded agencies.

Agencies under the policy authority, but not directly managed by DoIT must independently comply with the requirements outlined within this policy.

This policy establishes the following requirements:

4.1 Boundary Control Devices

Agency information technology and cybersecurity staff shall monitor and control all network boundaries using boundary control devices in a defense-in-depth capacity (e.g. firewalls, routers, proxy servers, etc.). All boundary control devices shall conform to established standards and configurations designated through DoIT configuration management processes. Agencies shall:

- Determine that all points of ingress/egress between network segments in the DoIT Enterprise and subordinate agency networks, or between the DoIT Enterprise and 3rd party networks including the Internet, are governed by a managed device or combination of devices (such as a firewall and a router) that share boundary control responsibilities
- At a minimum, ensure there are boundary devices that are capable of and configured to perform:
  - Source and destination address filtering
  - Network and port address translation
  - **Stateful inspection**
- Ensure that all firewalls are configured for event logging. Logs must be stored and retained based on the agency's retention policy, and analyzed daily for malicious/anomalous activities or errors (See *Continuous Monitoring Policy*)
- Ensure that all boundary control devices shall be identified and maintained as inventory in accordance with the *Asset Management Policy*.

4.2 Publicly Accessible Systems

Any agency maintaining or deploying any publicly accessible IT Systems not managed by the DoIT Enterprise shall ensure these systems and services are configured with standardized security controls established and maintained through DoIT configuration management processes (See *Configuration Management Policy)*. This process determines the minimum controls needed to protect the confidentiality, integrity, and availability of publicly accessible information, applications, and data.

Publicly Accessible Systems shall not store **confidential information** within the untrusted portions of a network, such as a **DMZ**. All publicly accessible, official, State websites and systems must use the most comprehensive cryptographic protocol available whenever possible (such as TLS 1.2 currently) to ensure data is protected while in transit.

4.3 Remotely Accessible Systems

Any IT Systems that are remotely accessible by users, such as **VPN** access or remote desktop service, will be governed by the *Remote Access Policy* and restricted to individuals authorized to access any internal IT Systems remotely.

4.4 Non-Publicly Accessible Systems

Non-Publicly Accessible Systems must be configured to remain undiscoverable from the public Internet, such as through reconnaissance tactics like ping sweeps, port scans or any other form of discovery, with the exception of the device(s) actually routing and/or firewalling between DoIT and the Internet.

4.5 Limitation of Access Points

The number of ingress/egress points for the DoIT Enterprise network, or subordinate agency networks, shall be limited to the minimum number necessary to accomplish an agency's mission and provide sufficient bandwidth for designated business objectives and contingencies.

Connecting any unauthorized boundary device, such as an unauthorized wireless access point to an internally networked computer, shall be considered a security violation.

4.6 Traffic Flow Rules

All ingress/egress points for the DoIT Enterprise network, or subordinate agency as well as all internal boundaries within that network, shall be governed by Traffic Flow Rules (such as firewall rules and access control lists) that are specific to each point of ingress/egress (or groups of points that abide by the same rules). These Traffic Flow Rules shall be an explicit documentation of each form of network traffic that is allowed through that point. Documented elements for each traffic type will be maintained through the configuration management approved baseline and shall include:

- Authorized protocol;
- Authorized sources and destinations;
- Authorized TCP/UDP ports if applicable;
- Authorized hours for usage, if limited;
- Authorized dates, if temporary;
- Required authentication mechanism, if required;
- Business purpose of allowed traffic; and
- Authorizing individual name and role.

4.7 Boundary Control Rule Sets

All devices that contain boundary control mechanisms shall be configured such that:

- All network traffic shall be denied by default through any boundary;
- If the device does not include an implicit deny function, then an explicit deny shall be configured in such a way that the same objective is achieved;
- All traffic allowed through the device must be explicitly allowed with specific rules;
- Specific allow rules shall be configured in compliance with the traffic policy for the boundary and shall be written as narrowly as possible to allow only the required traffic.

4.8 Failure of Boundary Protection

In the event of a failure in key boundary protection mechanisms, boundary protection devices will fail CLOSED where this is a configurable option. This ensures connectivity through the devices is disabled and helps to prevent exploitation and loss of monitoring capability. Boundary protection products that only fail OPEN should be avoided where possible.

4.9 Internet Access

Internet access shall be allowed under the following conditions:

- Where possible, all web browsing traffic must be:
    - Assessed for protocol compliance, and dropped if non-compliant;
    - Compared against blacklists of unauthorized host names, URL elements, HTTP host headers, or other fields relevant to the associated protocol, and dropped if there is a match. Refer to the configuration management documentation for information such as whitelists, blacklists, and URL content filtering; and
    - Processed through a web-proxy, where applicable.
- All outbound traffic shall be monitored for unauthorized content;
- All Internet access by employees must conform to the DoIT *Acceptable Use Policy*.

4.10 Continuous Monitoring

All boundary devices and traffic flow will be subject to the DoIT *Continuous Monitoring Policy* and *Audit and Compliance Policy*. This policy specifies that all boundary protection controls be configured to allow authorized personnel to monitor and protect the network against malicious code, denial of service, intrusions, and insider threats.

4.11 Management of Boundary Control Devices

Management of boundary control devices should be conducted according to the following mechanisms:

- All DoIT-managed firewalls must be located in secured rooms accessible only to those authorized by management to have access;
- All default administrator credentials shall be changed including **SNMP** strings (disable SNMP if not used);
- Only IT staff authorized to access boundary control devices shall be granted such access; and
- IT staff shall not use shared administrative accounts, but will be granted user-specific accounts.

4.12 Change Controls

Changes applied to boundary control devices or architectures must be approved in accordance with the *Configuration Management Policy* change management processes regardless of whether or not the change is a temporary or permanent configuration change.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an agency under the policy authority of DoIT requires an exemption from this policy then that agency must submit a DoIT Policy Exemption Request Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Other related policies include:

- Acceptable Use Policy
- Audit and Compliance Policy
- Configuration Management Policy
- Continuous Monitoring Policy
- Physical & Environmental Protection Policy
- Public and Confidential Information Policy
- Remote Access Policy
- Wireless Access Policy

7.0 Definitions

Term	Definition
Confidential Information	Confidential information is considered non-public information and is defined as Personally Identifiable Information (PII), Privileged Information, and Sensitive Information. See *Public and Confidential Information Policy*.
De-militarized Zone (DMZ)	Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.
Firewall	A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures.
Non-Publicly Accessible Systems	Any system, application, or service accessed by State employees, contractors, vendors, or other authorized entities through an internal, authenticated process restricted to internal network access only, such as logging into a domain authenticated computer.
Publicly Accessible Systems	Any system, application, or service used as a resource by the residents and/or constituents of the State of Maryland or external interested parties (such as the Department of Tourism's web pages containing the Calendar of Events).
Remotely Accessible Systems	Any system, application, or service accessed by State employees, contractors, vendors, or other authorized entities from an external connection to any internal

Term	Definition
	resource to administer or to operate an internal resource, such as connections made through VPN.
Secure Sockets Layer (SSL)	A protocol used for protecting private information during transmission via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most Web browsers support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https://” instead of “http://”.
Simple Network Management Protocol (SNMP)	An Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.
Stateful Inspection	A firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through a firewall. Also known as dynamic packet filtering.
Virtual Private Network (VPN)	A virtual network, built on top of existing physical networks that provides a secure communications tunnel for data and other information transmitted between networks.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for managing boundary control assets for Enterprise onboarded agencies. DoIT will manage the devices according to established requirements authorized in the DoIT Cybersecurity Program Policy and described in this policy’s Section 4.0. Agencies not directly managed by DoIT must exercise due diligence and due care to comply with the minimum standards identified by the relevant DoIT policies. Any agencies under the policy authority of DoIT with requirements that deviate from the DoIT Cybersecurity Program policies are required to submit a Policy Exemption Form to DoIT for consideration and potential approval.

If DoIT determines that an agency is not compliant with this policy, the agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After which, the Secretary of Information Technology, or a designated authority, may extend a non-compliant agency’s window of resolution or authorize DoIT to shutdown external and internal network connectivity until such time the agency becomes compliant.

Any attempt by personnel to circumvent or otherwise bypass this boundary protection policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written notice, suspension, termination, and possibly criminal and/or civil penalties.